



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

March 14, 2012

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2012-015

DATE(S) ISSUED:

3/14/2012

SUBJECT:

Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client.

Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or bypass security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Firefox versions prior to 3.6.28, ESR 10.0.0.3, and 11.0
- Thunderbird versions prior to 3.1.20, ESR 10.0.0.3, and 11.0
- SeaMonkey versions prior to 2.8

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High**DESCRIPTION:**

Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey. The details of these vulnerabilities are as follows:

Security Bypass Vulnerability

Several unspecified security bypass vulnerabilities have been discovered in Firefox, Thunderbird, and SeaMonkey. These vulnerabilities can be exploited to bypass security restrictions and allow for spoofing in the user interface.

Cross-Site Scripting Vulnerability

Two unspecified cross-site scripting vulnerability have been discovered which allow arbitrary script code to be executed in the browser of an unsuspecting user. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

Information Disclosure Vulnerability

An information disclosure vulnerability has been discovered that can disclose sensitive data from the user's memory.

Remote Memory Corruption Vulnerability

Multiple unspecified memory corruption vulnerabilities can occur when navigating to a specially crafted web page. When this vulnerability is exploited, it may result in remote code execution. Failed exploit attempts will most likely cause a denial-of-service of the application.

Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or bypass security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade vulnerable Mozilla products immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:**Mozilla:**

<http://www.mozilla.org/security/announce/2012/mfsa2012-13.html>

<http://www.mozilla.org/security/announce/2012/mfsa2012-14.html>

<http://www.mozilla.org/security/announce/2012/mfsa2012-15.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-16.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-17.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-18.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-19.html>

SecurityFocus:

<http://www.securityfocus.com/bid/52455>
<http://www.securityfocus.com/bid/52456>
<http://www.securityfocus.com/bid/52457>
<http://www.securityfocus.com/bid/52458>
<http://www.securityfocus.com/bid/52459>
<http://www.securityfocus.com/bid/52460>
<http://www.securityfocus.com/bid/52461>
<http://www.securityfocus.com/bid/52463>
<http://www.securityfocus.com/bid/52464>
<http://www.securityfocus.com/bid/52465>
<http://www.securityfocus.com/bid/52466>
<http://www.securityfocus.com/bid/52467>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0454>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0456>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0462>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0460>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0459>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0455>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0457>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0458>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0451>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0461>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0464>